

Posudek vedoucího bakalářské práce

Název práce: The use of symbolic execution for testing of real-time safety-critical software

Jméno autora: Martin Hořeňovský

Vedoucí práce: Ing. Michal Sojka, Ph.D.

Katedra řídicí techniky, FEL, ČVUT

Cílem této práce bylo ověřit praktickou použitelnost verifikace softwaru metodou symbolické exekuce. Hlavním přínosem této metody je, že v ideálním případě projde všechny možné cesty programem a najde tak chyby, které se vyskytují ve zřídka vykonávaných cestách, například v kódu pro obsluhu běhových chyb. To je důležité právě u bezpečnostně-kritického softwaru, na jehož správném fungování ve všech situacích často závisí lidské životy.

Původně bylo v plánu, že pan Hořeňovský bude verifikovat „produkční“ bezpečnostně-kritický software poskytnutý firmou Infineon. Z toho ale nakonec sešlo, zejména kvůli odkladu odevzdání bakalářské práce za konec projektu s touto firmou. Místo toho jsme pro verifikaci zvolili implementaci komunikačního protokolu MaCAN, u kterého se také uvažuje o nasazení v bezpečnostně-kritických aplikacích.

Student pracoval samostatně, ale podle mého názoru poměrně pomalu. Hned po zadání práce se začal seznamovat s nástrojem Klee a ze své iniciativy začal navrhopvat jeho možná vylepšení, ale k vlastní verifikaci zadaného kódu se ne a ne dostat. Poté se student zhruba na rok odmlčel a v práci pokračoval až v semestru před odevzdáním. Bohužel ani tuto závěrečnou fázi si pan Hořeňovský nezorganizoval ideálně a většinu práce odvedl na poslední chvíli před odevzdáním.

Pominu-li časový aspekt, pracovalo se mi se studentem velmi dobře. Konzultace byly věcné, student se řídil mými pokyny a doporučeními a výsledek práce odpovídá mému očekávání. Myslím si ale, že by pan Hořeňovský měl na víc. Je to bezpochyby bystrý a šikovný student a kdyby si práci lépe zorganizoval, jistě by v ní pokročil dále a dosáhl by zajímavějších výsledků.

Práci navrhuji hodnotit stupněm B – **velmi dobře**.

V Praze dne 3. června 2015

Ing. Michal Sojka, Ph.D.